TMA Privacy and Civil Liberties Office Information Paper

ORAL COMMUNICATION OF PHI

HIPAA Privacy ◆ March 2010

PURPOSE

General Requirement

The Department of Defense Health Information Privacy Regulation, DoD 6025.18-R, applies to Protected Health Information (PHI) in all forms —electronic, written, oral, and any other non electronic forms. The application of privacy standards to oral (spoken) information ensures protection when discussed, or read aloud from a computer screen or a written document. HIPAA protects oral communication between health care providers and to their patients by establishing guidelines for appropriate modes of communication.

GUIDANCE

Confidential Communication With Other Providers

The Privacy Regulation is not intended to prohibit providers from talking to each other and to their patients; however, provisions of this Regulation do require covered entities to implement reasonable safeguards that reflect their particular circumstances. Within the Regulation, C8.4 provides further guidance regarding incidental uses and disclosures which includes the occurrence of conversations among healthcare providers or with patients when there is a possibility of being overheard. For example, in a busy emergency room, it may be necessary for providers to speak loudly in order to ensure appropriate treatment. The following practices are permissible, if reasonable precautions are taken to minimize the chance of unintentional disclosures to others who may be nearby (such as using lowered voices or talking away from others):

- Health care staff may orally coordinate services at hospital nursing stations.
- Nurses or other health care professionals may discuss a patient's condition over the phone with the patient, a provider, or a family member.
- A health care professional may discuss lab test results with a patient or other provider in a joint treatment area.
- A physician may discuss a patient's condition or treatment regimen in the patient's semi-private room.
- Health care professionals may discuss a patient's condition during training rounds in an academic or training institution.

- A pharmacist may discuss a prescription with a patient over the
- Pharmacy counter or with a physician or the patient over the phone.

Reasonable Safeguards

Covered entities must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI. "Reasonable safeguards" means that covered entities must make reasonable efforts to prevent uses and disclosures not permitted by the Regulation. In determining what is reasonable, potential effects on patient care, financial burden and other such concerns should be taken into account.

For example, the Privacy Regulation does not require the following types of structural or systems changes:

- Private rooms.
- Soundproofing of rooms.
- Encryption of wireless or other emergency medical radio communications.
- Encryption of telephone systems.

Examples of the types of adjustments or modifications to facilities or systems that may constitute reasonable safeguards are:

- Pharmacies could ask waiting customers to stand a few feet back from a counter used for patient counseling.
- Providers can speak quietly and avoid using patients' names in a waiting room, public hallways, elevators, and any other public areas.
- Providers could add curtains or screens to areas where oral communication often occur between doctors and patients or among professionals treating the patient.
- In an area where multiple patient-staff communication routinely occurs, use of cubicles, dividers, shields, or similar barriers may constitute a reasonable safeguard.

Minimum Necessary

When using or disclosing PHI in any form, including oral communication, a covered entity shall make reasonable efforts to limit the use, disclosure, or request of PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The minimum necessary standards, found under section C8.2, are intended to make covered entities evaluate their practices and enhance protections as needed to limit unnecessary or inappropriate disclosures of PHI. This does not apply to uses or disclosures for which an authorization was obtained, an exchange among providers for treatment purposes, or patient to provider communication.

Documentation of Oral Communication

The Privacy Regulation does not require covered entities to document any information, including oral information that is used or disclosed for treatment, payment or health care operations (TPO). There are, however, documentation requirements for some information disclosures for other purposes. For example,

some disclosures must be documented in order to meet the standard for providing a disclosure history to an individual upon request. The Protected Health Information Management Tool (PHIMT) is the web based tool of choice for documenting disclosures of PHI across the MHS. All the above requests for PHI should be documented and tracked using the PHIMT. Information regarding training on the PHIMT is available from the Privacy website at http://www.tricare.mil/tma/privacy/ProtectedHealthInformationManagementTool.aspx.

The local MTF Privacy Officer is responsible for ensuring proper training of the application and use of the PHIMT is accomplished.